Advisory Services
Security

Respected—but still restrained

In the aftermath of the worst global economic jolt in 30 years, information security confronts a new economic order.

Findings from the 2011 Global State of Information Security Survey®

PricewaterhouseCoopers

Methodology

The 2011 Global State of Information Security Survey® is a worldwide security survey by PricewaterhouseCoopers, *CIO Magazine* and *CSO Magazine*. It was conducted online from February 19, 2010 to March 4, 2010. Readers of *CIO* and *CSO Magazines* and clients of PricewaterhouseCoopers from around the globe were invited via email to take the survey. The results discussed in this report are based on the responses of more than 12,840 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 135 countries. Thirty-seven percent of respondents were from Asia, 30% from Europe, 17% from North America, 14% from South America, and 2% from the Middle East and South Africa. The margin of error is less than 1%.

Table of contents

The heart of the matter

As global economic conditions continue to fluctuate, information security hovers in the balance – caught between a new hard-won respect among executives and a painstakingly cautious funding environment.

Over the past year, it has been hard to predict when, where and with what strength global economic conditions might improve.

So it isn't surprising to discover this year, that—according to the results of the 2011 Global State of Information Security Survey®—executives across industries and markets worldwide have been reluctant to release funding to support the information security function.

This financial restraint is in spite of clear evidence that as information security emerges from the smoke of a brutal year—and, in effect a "trial by fire," as last year's survey revealed—it is sporting a new hard-won respect, not just from many but from most of this year's respondents. This includes more than 12,800 CEOs, CFOs, CIOs, CISOs, CSOs and other executives responsible for their organization's IT and security investments in more than 135 countries.

As the spending restraint continues, however, some "block and tackle" security capabilities that took a full decade to develop are degrading and, day by day, opening up organizations to new windows of risk.

This year, the tension is acute. Between ongoing maturation in the security function and regression. Between caution in this economy and optimism. Between preserving cash and protecting the business.

Caught in the balance is the information security function—thirsty for funds and poised to continue systematically driving into the heart of the business.

What is the evidence of these trends? What are the implications for spending during the next six to 12 months? Where are the greatest security-related vulnerabilities emerging? And which are the most crucial opportunities and priorities your organization should focus on now and over the next year to increase the contribution that security makes to your business?

An in-depth discussion

Signs of security's strategic gains and advances stand side by side with newly emerging cracks in its foundation.

I. Spending: A subtle but enormously meaningful shift

Finding #1
Three strategic trends in spending—each of them several years in the making—are now hard to miss.

Finding #2
This year's spending drivers aren't new. But here's the surprise: Almost every one of these factors are trending at, or near, four-year lows.

Finding #3
Client requirement has now emerged—either as the new "flavor of the year" or perhaps as a strategic driver of spending that will endure over time.

Finding #1. Three strategic trends in spending—each of them several years in the making—are now hard to miss.

Look at these numbers over a multi-year period. This year—for the first time in the course of the survey—three long-term strategic trends in information spending have appeared in the spotlight.

1. Security is on the CFO's "protect" list
We first saw evidence of this last year. This year's data provides additional confirmation of the trend. As the function matures—and contributes in more obvious and direct ways to business objectives—it is encountering much more stable funding curves. As the survey revealed last year, security funding is protected during the "down" cycle. And—as we will point out in the pages that follow—this funding is increased as market vigor returns.

2. Yet security is still vulnerable to the "flavor of the year"
Because security sits at the heart of the business, its spending drivers—the factors emphasized most prominently and most often by executives seeking funding for security-related initiatives—tend to be very closely aligned with the "hot priorities" of the business, whatever they might be at the time. In short, security's spending drivers are susceptible to what we might call the "flavor of the year."

Take the US market, for example. In 2007, six years after the events of 9/11, 68% of US respondents identified business continuity and disaster recovery as the single largest driver of security spending, compared with 43% today. In the same year—five years after the passage of the Sarbanes-Oxley Act and two years after the Health Insurance Portability and Accountability's (HIPAA) Security Rule took effect—US respondents identified regulatory compliance as the second-greatest spending driver, compared with 47% today.

3. The "water drop" effect
Big splash – then diffusion. After peaking as drivers, each of these factors, from business continuity to regulatory compliance, shifts from an "external game-changer" to an "internal given." They remain important to the organization—often crucially so—but precisely because of their value, they become integrated into the business. How? Through, for example, newly automated systems or feature-enhanced software. Updated job descriptions. Policies and business practices. And more comprehensively designed internal controls.

Finding #2. This year's spending drivers aren't new. But here's the surprise: Almost every one of these factors are trending at, or near, four-year lows.

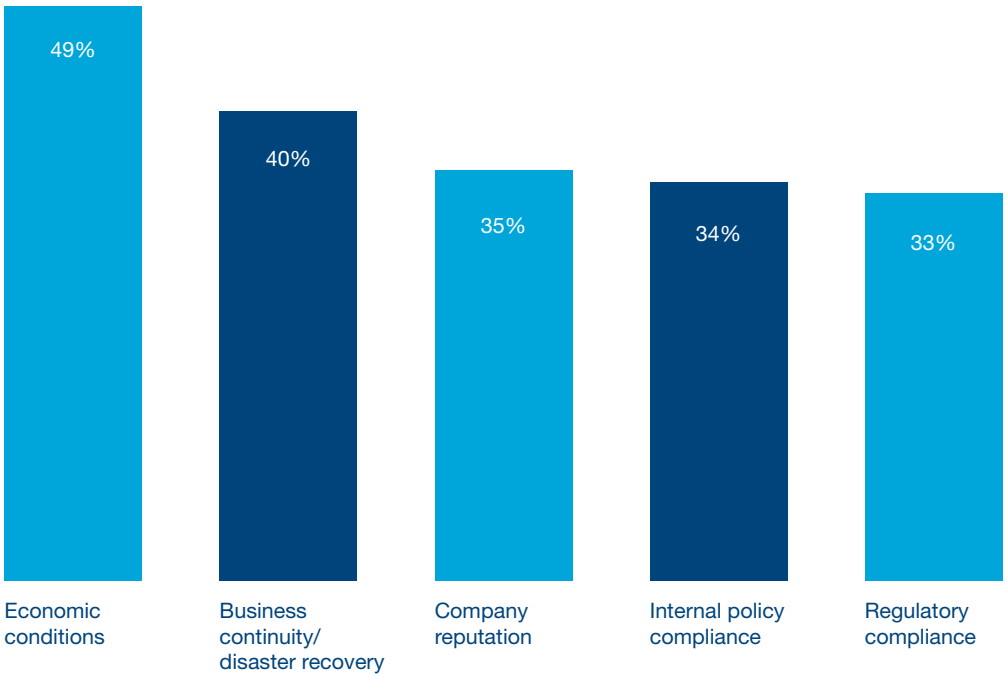
Which factors are driving information security spending this year? At first glance, the answer isn't much of a shock: economic conditions (reported by 49% of respondents), business continuity and disaster recovery (40%), company reputation (35%), internal policy compliance (34%) and regulatory compliance (33%). (Figure 1)

These are the primary factors you would expect—not just one year after the greatest economic downturn in the last 30 years but also after a decade of expanding globalization; continual introduction of new technologies that enable a free flow of information worldwide; the introduction of the Advanced Persistent Threat; and a wave of regulation across markets, industries and regions.

What is surprising, however, is that almost every one of these factors is trending at or near four-year lows. Take business continuity/disaster recovery, for example. Sixty-eight percent of respondents pointed to this factor just four years ago. That was 28 points ago—a reduction of 41% compared with this year. The other drivers show comparable declines. (Figure 2)

First, let's clarify a key issue: Does this mean these factors are *less important*? Absolutely not. In many respects, they've never been more vital. They're just not as vigorous spending drivers as they've been in the past.

Figure 1: Percentage of respondents who identify the following business issues or factors as the most important drivers of information security spending in their organization. [1]



[1] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

Figure 2: Percentage of respondents who identify the following business issues or factors as the most important drivers of information security spending in their organization. [2]

	2007	2008	2009	2010	Three-year % change*
Economic conditions	n/a	n/a	39%	49%	n/a
Business continuity/disaster recovery	68%	57%	41%	40%	-41%
Company reputation	44%	39%	32%	35%	-20%
Internal policy compliance	51%	46%	38%	34%	-33%
Regulatory compliance	54%	44%	37%	33%	-39%

[2] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.
* This calculation measures the difference between response levels over a three-year period from 2007 to 2010.

Source: The 2011 Global State of Information Security Survey®

Finding #3. Client requirement has now emerged—either as the new "flavor of the year" or perhaps as a strategic driver of spending that will endure over time.

What is the new "flavor of the year"? Client requirement—although the meaning of this term likely varies a bit across respondents.

This year, when respondents were asked how information security spending was justified in their organization, nearly every one of the top seven factors they identified—from common industry practice to potential liability or revenue impacts—reflected declines in comparison with 2007. The reductions ranged from 10% to 26%.

Client requirement was not only the sole factor in the top seven to increase over this period, it also moved up in ranking from the bottom of the list (#6 position) to near parity (#2 position) with the leading factor: justification for information security. (Figure 3)

Does client requirement refer to an internal client or an external one? A contractual mandate or a minimal threshold on a request for proposal? While the survey is ambiguous on this point, it's abundantly clear that "client requirement" in general is driving spending more than it ever has in the past.

Is client requirement just the new "flavor," or will it prove to be a more enduring driver? Could client requirement become the globally acknowledged leading driver of security spending in the next three to four years?

Perhaps. At this point it appears to be one more sign that, after 15 years, the information security function continues to take on a far more customer-facing, business-supporting, strategic value-building role.

Figure 3: Percentage of respondents who identify the following factors when asked to reveal how information security is justified in their organization. [3]

	2007	2008	2009	2010	Three-year % change*
Legal/regulatory environment	58%	47%	43%	43%	-26%
Client requirement	34%	31%	34%	41%	+21%
Professional judgment	45%	46%	40%	40%	-11%
Potential liability/exposure	49%	40%	37%	38%	-22%
Common industry practice	42%	37%	34%	38%	-10%
Risk reduction score	36%	31%	31%	30%	-17%
Potential revenue impact	30%	27%	26%	27%	-10%

[3] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.
* This calculation measures the difference between response levels over a three-year period from 2007 to 2010.

Source: The 2011 Global State of Information Security Survey®

II. Economic context: The leading impacts and strategies

Finding #4
While the impacts of the downturn linger, the largest increase in risk is associated with weaker partners and suppliers.

Finding #5
The strategies companies are taking this year are largely the same as those taken last year. Some of these strategies, however, may be opening up companies to new areas of risk.

Finding #4. While the impacts of the downturn linger, the largest increase in risk is associated with weaker partners and suppliers.

While a robust return to economic strength has been elusive, most economists agree that market conditions today are far better than they were in late 2008. So it's natural to expect that executive perceptions of the impacts the downturn has had on the security function would be different than they were last year.

They're not. At least most of them aren't. In fact, they're surprisingly consistent with last year's. Most agree, for example, that the regulatory environment has become more complex and burdensome. And that the increased risk environment continues to elevate the importance of the security function. And that ongoing cost-reduction efforts make adequate security more difficult to achieve. (Figure 4)

So what's the greatest change reported in the global economy's impact to the function this year? Respondents are considerably more likely than last year to report that business partners and suppliers have been weakened by economic conditions.

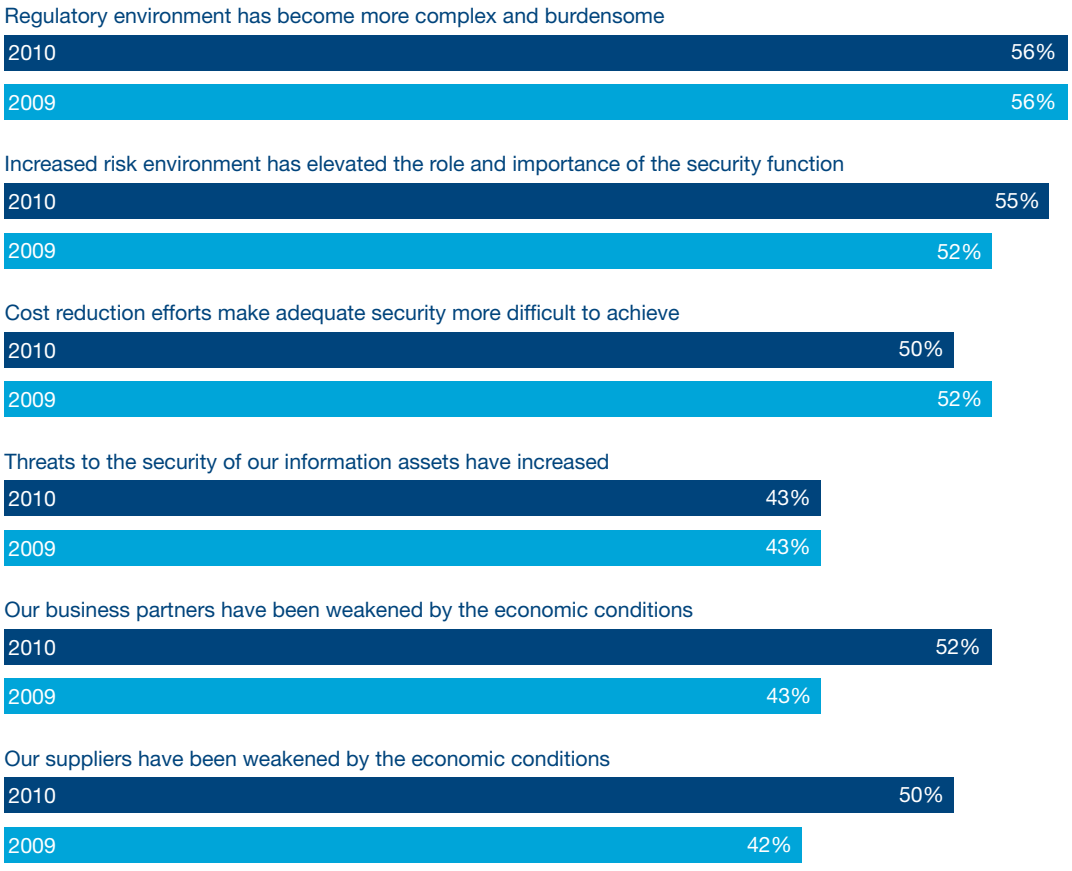
That's understandable, especially given factors such as the recent surge in globalization and cross-border participation in supply chains and emerging market development as well as the fact that one would naturally expect the real impacts to partners and suppliers to take at least one year to emerge.

But there's a much less obvious implication here, one that is enormously revealing about the strategic evolution in the maturity of the security function.

This data isn't just coming from senior business and IT decision-makers. Clearly, this information is also coming from—either directly or indirectly—core business managers at the center of companies and their operations. This includes the business unit heads, the operational decision-makers, the supply chain experts who work most closely with the organization's business partners and suppliers.

In other words, this year, we're starting to see quantitative evidence of anecdotal trends we have been tracking for several years: That the spotlights on security's value are turned on and shining brightly not just at the C-suite level but also at the very heart of organizational operations, in areas such as production, supply chain, procurement, business development and strategic partnering.

Figure 4: Percentage of respondents reporting the following impacts of current economic conditions on their organization's information security function. [4]



[4] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

Finding #5. The strategies companies are taking this year are largely the same as those taken last year. Some of these strategies, however, may be opening companies to new areas of risk.

Consider the strategies organizations are engaging to continue meeting security objectives in the face of this year's uncertain economic conditions. (Figure 5)

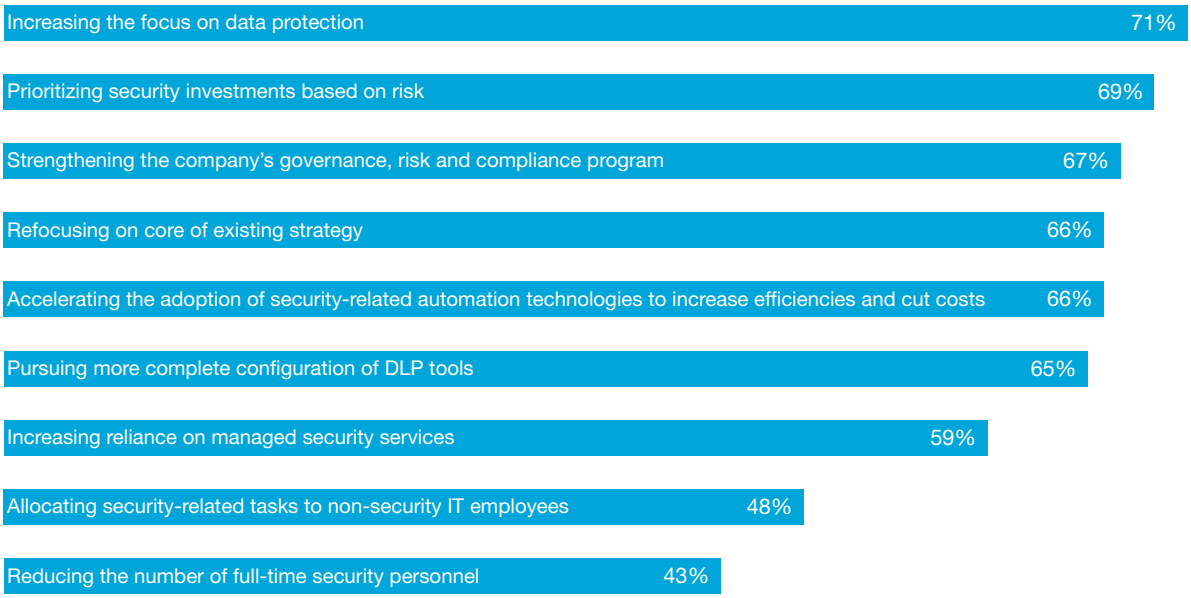
For the second year in a row, increasing the focus on data protection is the single most common strategy worldwide. Also consistent with last year's results are other priorities—such as prioritizing security investments based on risk; strengthening the company's governance, risk and compliance program; and accelerating the adoption of security-related automation technologies to increase efficiencies and cut costs.

Yet a second set of trends includes other strategies. Such as increasing reliance on managed security services. Reducing the number of full-time security personnel. And shifting security-related responsibilities to non-security personnel.

The business rationale behind these tactics, of course, is based on the need for greater efficiencies and a more reliable supply of more diversified security-related skills. Like IT, security needs to lower the cost of ongoing operations and devote more of the budget to new value-creation activities. But at the same time—and this is critical—these tactical strategies, in some cases, may be opening up organizations to new areas of risk.

For example, if companies are increasing their reliance on managed security services providers, are they also (1) enhancing governance and oversight mechanism, (2) conducting periodic audits of the provider's operations, and (3) ensuring the alignment of the provider's processes with the company's security policies, regulatory mandates and strategic risk management priorities?

Figure 5: Percentage of respondents reporting that, in order to meet their security objectives in the context of the harsh economic realities, the following strategies are important. [5]



[5] Respondents who answered "Important," "Very Important" or "Top Priority." Not all responses included. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

III. Funding and budgets: A balance between caution and optimism

Finding #6
Financial caution remains high as executives in the industry keep a tight lid on the budgetary coffers—at least for now.

Finding #7
Yet this caution appears to be easing for projects more than six months out and for reductions of 10% or more.

Finding #8
Asked about their expectations about security spending in the coming year, respondents are more optimistic than at any time since before 2005.

Finding #6. Financial caution remains high as executives in the industry keep a tight lid on the budgetary coffers—at least for now.

Funding is still tight. There's no question about it. Although some industries and markets appear to be strengthening, companies are reacting with extreme caution.

Asked whether their organization had reduced budgets for security initiatives over the last year, nearly half of all 12,847 respondents agreed that they had—for capital (47%) and operating expenditures (46%). And, in fact, these numbers matched last year's responses to the same question—(47% and 46% respectively). (Figure 6)

Quite surprisingly (at least given the signs of an impending market return to healthy levels of growth), more respondents than last year reported that their organization had deferred security-related funding for capital expenditures (from 43% in 2009 to 46% this year) and operating expenditures (from 40% to 42%).

A subtle tightening of the purse strings? Yes, apparently. A sign of even greater funding restraint to come? Perhaps. But not likely. Evidence suggests this hyper-focus on costs, in some cases, might be akin to one segment of the global consumer market's aversion to spending money in the months immediately preceding their purchase of a new car. Saving now in anticipation of spending later.

Figure 6: Percentage of survey respondents who report that their organization is reducing budgets for security initiatives or deferring them.

Has your company reduced budgets for any security initiatives?	2009	2010
Yes, for capital expenditures	47%	47%
Yes, for operating expenditures	46%	46%

Has your company deferred security initiatives?	2009	2010
Yes, for capital expenditures	43%	46%
Yes, for operating expenditures	40%	42%

Source: The 2011 Global State of Information Security Survey®

Finding #7. Yet this caution appears to be easing for projects more than six months out and for reductions of 10% or more.

In the seconds after the wheel of a fast-moving 200-ton ocean-transport vessel directs the ship in a markedly different direction—and before the evidence of this turn is apparent to the ship's compass—the water level on one side of the wave-cutting bow registers an unmistakable change.

That's happening here—so to speak. We took a closer look at how respondents answered our question about spending restraint for capital and operating expenditures. And what we discovered is quite fascinating.

Spending caution appears to be "easing" for projects more than six months out and for reductions of 10% or more. And it's "building up at the bow" for projects under six months or budget reductions under 10%.

Why is demand "bunching up" for near-term projects? It's hard to tell. Some of our clients are concerned about the short-term reliability and calendar timing of the return to economic strength. Others are interested in funding a higher portion of security-related investments in operating and capital expenditures from actual revenue streams as they manifest themselves on a cash basis, rather than accrual. And many management teams, of course, have their heads down trying to balance security's demand for those funds against "first distribution" calls for value-creating funding from across the enterprise.

How do we view this trend in the data? As a noteworthy shift in the focus of funding restraint—away from long-term initiatives and increasingly concentrated on initiatives planned for the short-term. We take that as an unimpeachable sign of cautious optimism—one sign, actually, of two.

Figure 7: Percentage of survey respondents who report that their organization is reducing budgets for security initiatives or deferring them.

Has your company reduced budgets for any security initiatives?	2009	2010	One-year change
Yes, for capital expenditures	47%	47%	
- by under 10%	19%	22%	+ 3 pts.
- by more than 10%	28%	25%	- 3 pts.
Yes, for operating expenditures	46%	46%	
- by under 10%	19%	22%	+ 3 pts.
- by more than 10%	27%	24%	- 3 pts.

Has your company deferred security initiatives?	2009	2010	One-year change
Yes, for capital expenditures	43%	46%	
- by less than 6 months	21%	27%	+ 6 pts.
- by more than 6 months	22%	19%	- 3 pts.
Yes, for operating expenditures	40%	42%	
- by less than 6 months	22%	26%	+ 4 pts.
- by more than 6 months	18%	16%	- 2 pts.

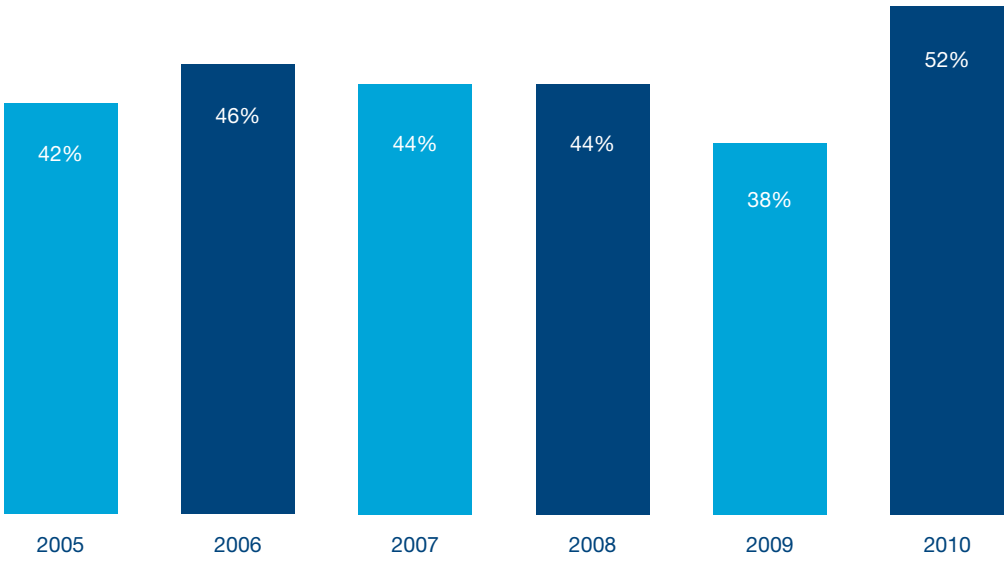
Source: The 2011 Global State of Information Security Survey®

Finding #8. Asked about their expectations about security spending in the coming year, respondents are more optimistic than at any time before 2005.

The second sign of optimism is a bit more exuberant. This year, expectations that spending will increase leaped by more points than at any time since the earliest years of this survey. This optimism—held by 52% of respondents, a higher number than any response level since before 2005—is significant. (Figure 8)

Absent another worldwide shock to the global economy, we may see a release of this pent-up demand "at the bow" and an increase in security-related spending on capital and operating expenditures as early as later this year.

Figure 8: Percentage of survey respondents who report that security spending will increase over the next 12 months. [6]



[6] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

IV. Capabilities and breaches: Trends too large to ignore

Finding #9
After posting solid advances in the last several years, some firms are allowing these capabilities to degrade.

Finding #10
As organizations continue to gain new visibility into security incidents, they are learning more about the real costs of breaches.

Finding #11
This year, there is a significant shift in the ongoing evolution of the CISO's reporting channel away from the CIO in favor of the company's senior business decision-makers.

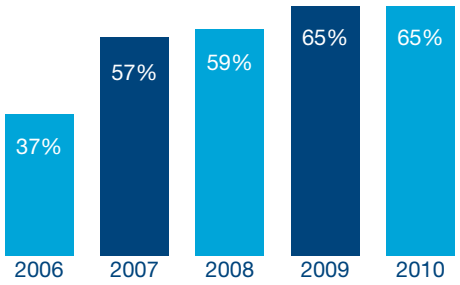
Finding #9. After posting solid advances in the last several years, some firms are allowing these capabilities to degrade.

This year, adoption levels for many information security-related processes appear to have stalled—an unplanned consequence, perhaps, of the austerity in the funding environment. Respondents are just as likely as they were last year, for example, to have an overall security strategy in place (65% in 2009, 65% this year), use vulnerability scanning tools (53% in 2009, 53% this year), and have wireless (cellular and Wi-Fi) security standards and procedures (45% in 2009, 45% this year). (Figure 9)

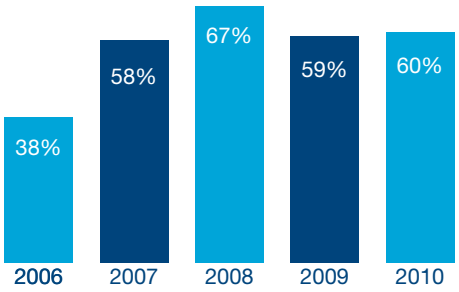
In many cases, however, these adoption rates are actually in decline. Fewer respondents compared with last year, for example, conduct personnel background checks (60% in 2009, 56% this year), dedicate people to monitoring employee use of the Internet and information assets (57% in 2009, 53% this year), and conduct an employee security awareness program (53% in 2009, 49% this year). (Figure 10)

Just a one-year impact? Maybe so. But where it occurs, this regression often returns these capabilities to 2008 levels or below.

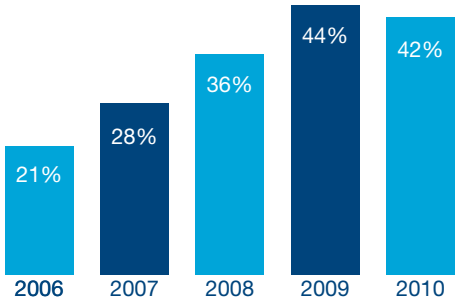
Figure 9: Percentage of survey respondents who report that their organization has the following security- and privacy-related capabilities in place. These sample responses highlight the fact that many capability advances have stalled. [7]



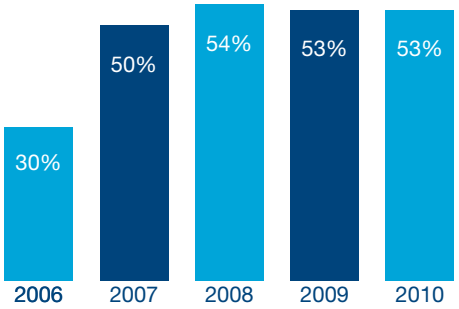
Have an overall information security strategy



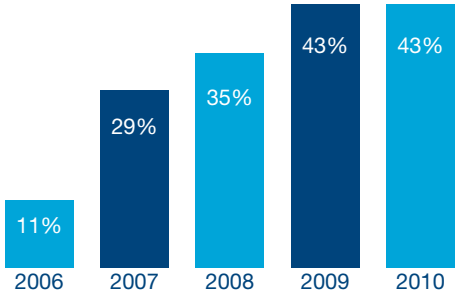
Ensure the secure disposal of technology hardware



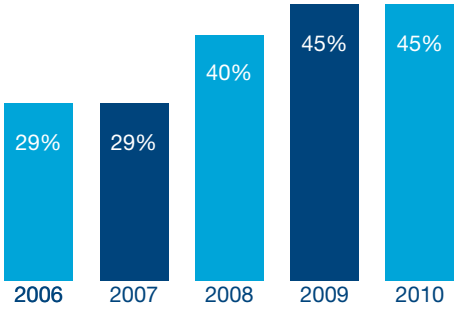
Integrate privacy and compliance plans



Use vulnerability scanning tools



Have implemented security event correlation software

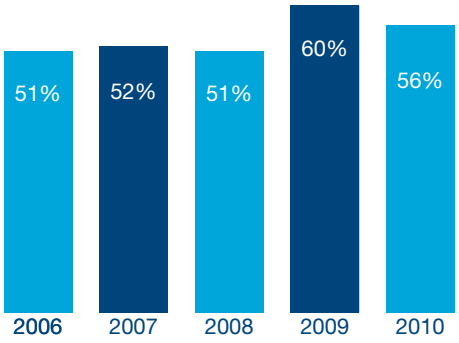


Have wireless (cellular and Wi-Fi) security standards and procedures

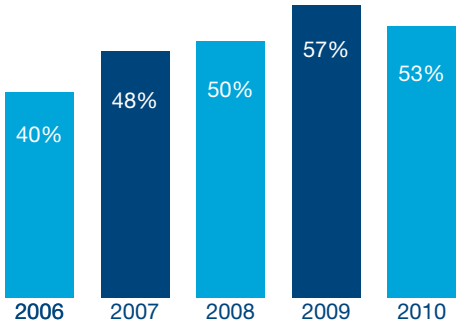
[7] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

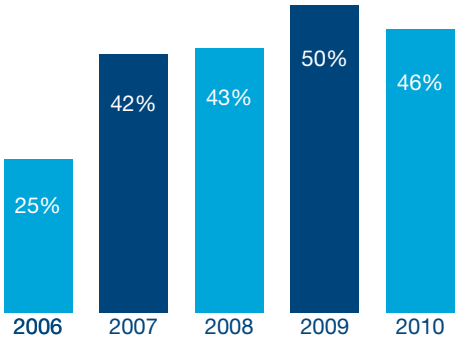
Figure 10: Percentage of survey respondents who report that their organization has the following security- and privacy-related capabilities in place. These sample responses reflect the emerging degradation in some capabilities. [8]



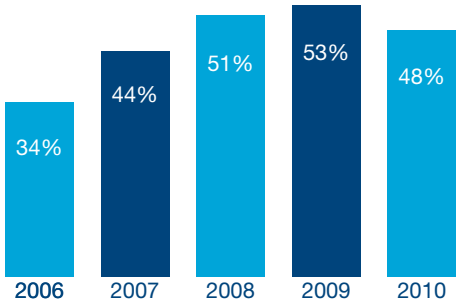
Conduct personnel background checks



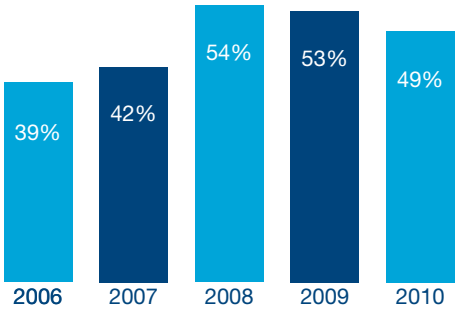
Have people dedicated to monitoring employee use of the Internet and information assets



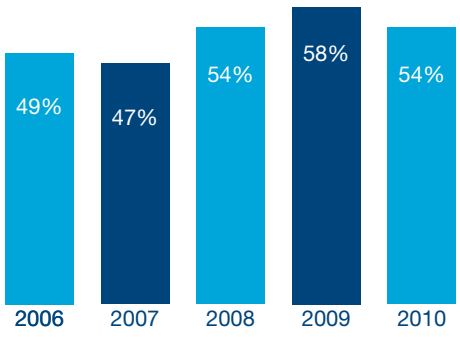
Have established security baselines for external partners, customers, suppliers and vendors



Use a centralized security information management process



Conduct an employee security awareness program



Actively monitor and analyze information security intelligence

[8] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

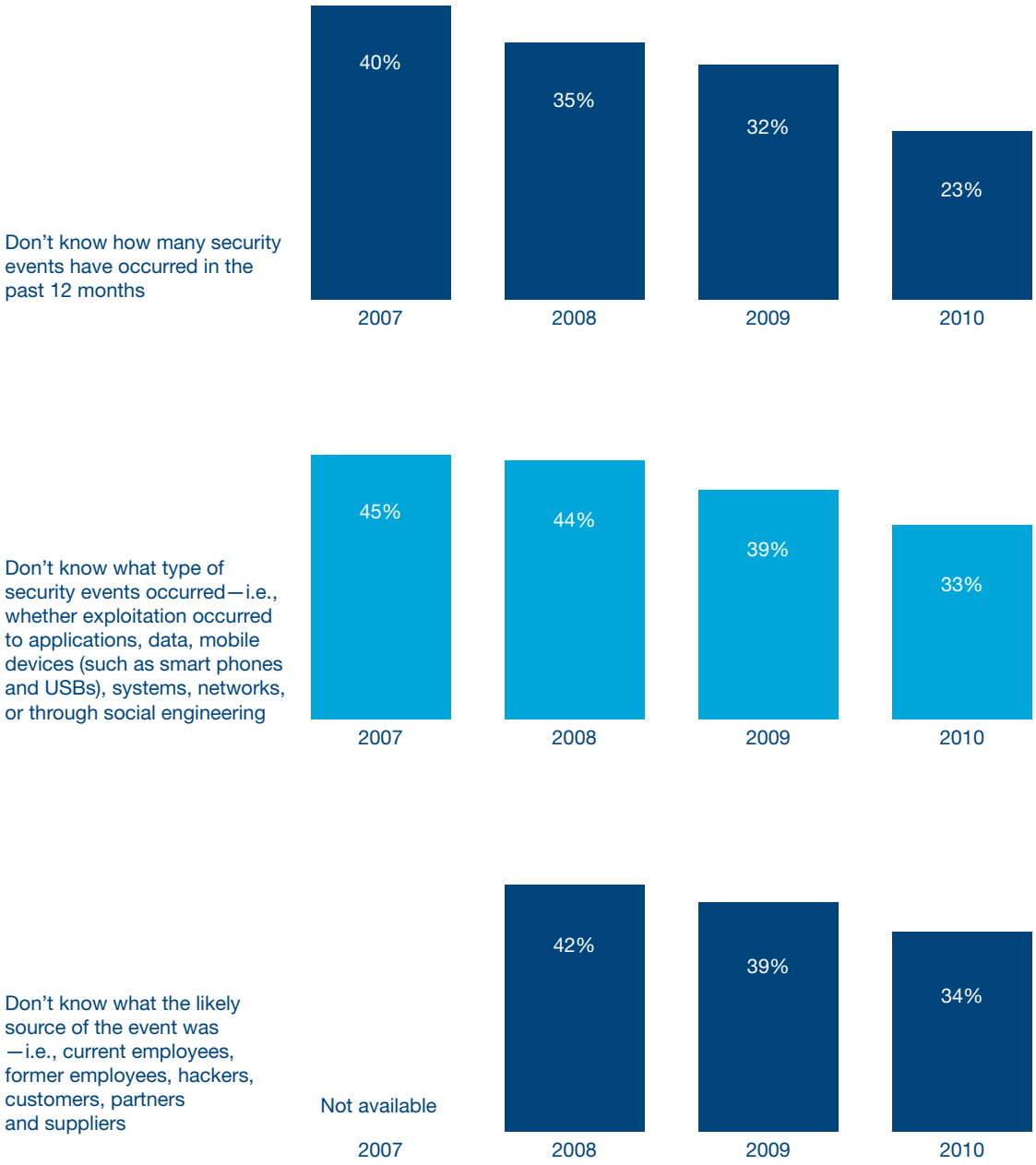
Finding #10. As organizations continue to gain new visibility into security incidents, they are learning more about the real costs of breaches.

For years, the percentages of respondents who reported not knowing about key security event-related facts have been painfully high. Just a few years ago in 2007, for example, 40% didn't know how many security events had occurred in the past 12 months. Today, 23% don't. In 2007, almost half (45%) didn't know what type of security events had occurred. Today 33% don't. (Figure 11)

As organizations continue to "turn on the lights," however, what they are finding is sobering. In short, the impact of security events on the business has risen to significant levels—particularly with respect to financial losses (now reported by 20% of all respondents), theft of intellectual property (15%) and compromises to brands or reputations (14%). (Figure 12)

As these numbers continue to rise, we foresee even greater pressure on the CFO to release funding—not just to maintain security capabilities at their current level but also to advance security's ability to protect and enable the business.

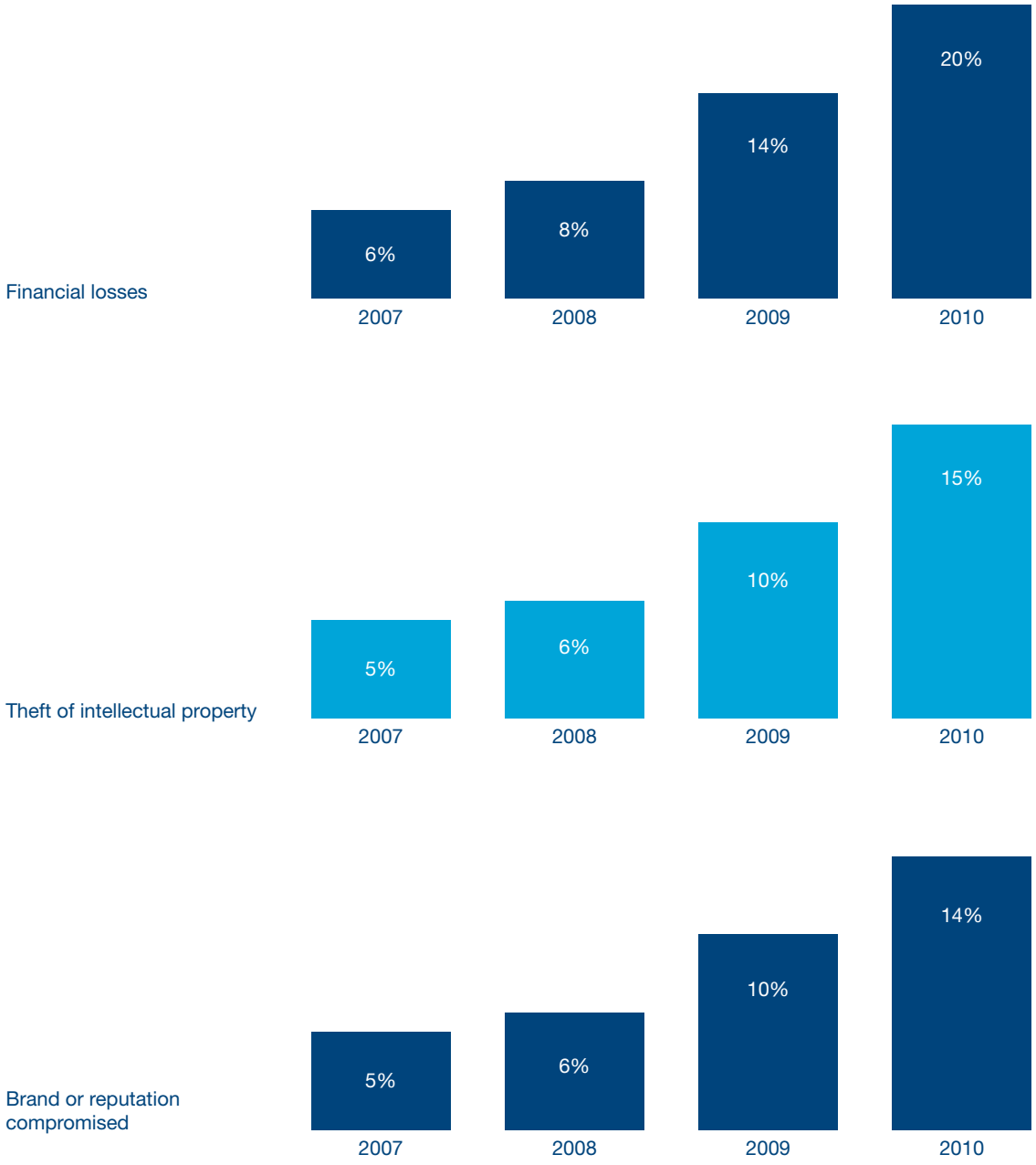
Figure 11: Percentage of survey respondents who report the following information with respect to negative security-related events impacting their organization. [9]



[9] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

Figure 12: Percentage of all survey respondents who report the following business impacts to their organization. [10]



[10] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

Finding #11. This year, there is a significant shift in the ongoing evolution of the CISO's reporting channel away from the CIO in favor of the company's senior business decision-makers.

The gap has widened. Three years ago, companies still viewed the information security function principally as a technology cost center. One unimpeachable sign of this was the fact that the single most common reporting channel for the Chief Information Security Officer (or equivalent information security executive) was to the Chief Information Officer.

How quickly the times have changed. Since 2007, the number of respondents reporting this viewpoint has declined very significantly, from 38% to 23% this year.

So where is the CISO reporting today? To the business "side of the house," typically to the Board, the CEO, the CFO, the Chief Operating Officer and the Chief Privacy Officer. (Figure 13)

What's the strategic significance of this reporting shift? Across industries, we continue to see evidence of executive recognition that security's strategic value is more closely aligned with the business than with IT.

Figure 13: Percentage of survey respondents who report that their organization's Chief Information Security Officer or equivalent information-security leader reports to the following senior executives. [11]

	2007	2008	2009	2010	Three-year % change*
Chief Information Officer (CIO)	38%	34%	32%	23%	-39%
Board of Directors	21%	24%	28%	32%	+52%
Chief Executive Officer (CEO)	32%	34%	35%	36%	+13%
Chief Financial Officer (CFO)	11%	11%	13%	15%	+36%
Chief Operating Officer (COO)	9%	10%	12%	15%	+67%
Chief Privacy Officer (CPO)	8%	8%	14%	17%	+113%

[11] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.
* This calculation measures the difference between response levels over a three-year period from 2007 to 2010.

Source: The 2011 Global State of Information Security Survey®

V. New areas of focus: Where the emerging opportunities lie

Finding #12
Not surprisingly, social networking represents one of the fastest emerging new areas of risk.

Finding #13
One of the leading priorities for many companies is mitigating the consequences of a breach—through better incident response.

Finding #14
A newly popular tool in the CISO's arsenal? Insurance.

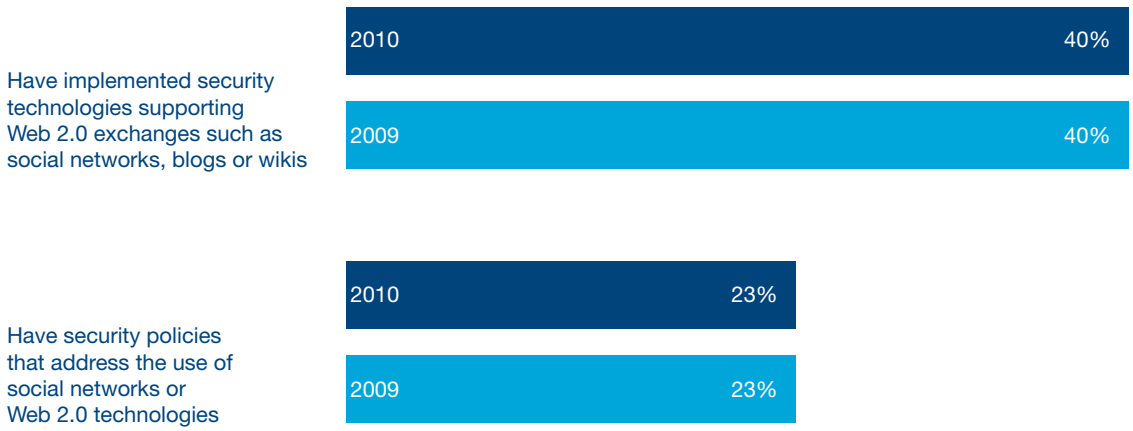
Finding #12. Not surprisingly, social networking represents one of the fastest emerging new areas of risk.

As if protecting data across applications, networks and mobile devices wasn't complex enough, social networking by employees is presenting organizations worldwide with a new and growing frontier of risk.

The risks, from an information security perspective, include the loss or leaking of information; statements or information that could damage the company's reputation; activity such as downloading pirated material with legal and liability implications; identity theft that directly and indirectly compromises the company's network and information; and data aggregation in building up a picture of an individual to mount security attacks through social engineering.

Few companies are adequately prepared to counter this threat. Most companies (60%) have yet to implement security technologies supporting Web 2.0 exchanges such as social networks, blogs or wikis. And even more (77%) have not established security policies that address the use of social networks or Web 2.0 technologies—a critical strategy that costs virtually nothing. (Figure 14)

Figure 14: Percentage of survey respondents who report that their organization has the following information security capabilities in place. [12]



[12] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

Finding #13. One of the leading priorities for many companies is mitigating the consequences of a breach—through better incident response.

At first glance, the nearly six out of every 10 (58%) respondents who report their organization has a contingency plan in place for security incidents is a healthy number. (Figure 15)

But when you factor this number by the percentage who report that their plan is effective (63%), the results are disheartening.

In effect, most organizations (63%) have no plan or the plan they have doesn't work.

Figure 15: Percentage of survey respondents reporting on whether or not their organization has a contingency plan to respond to incidents.

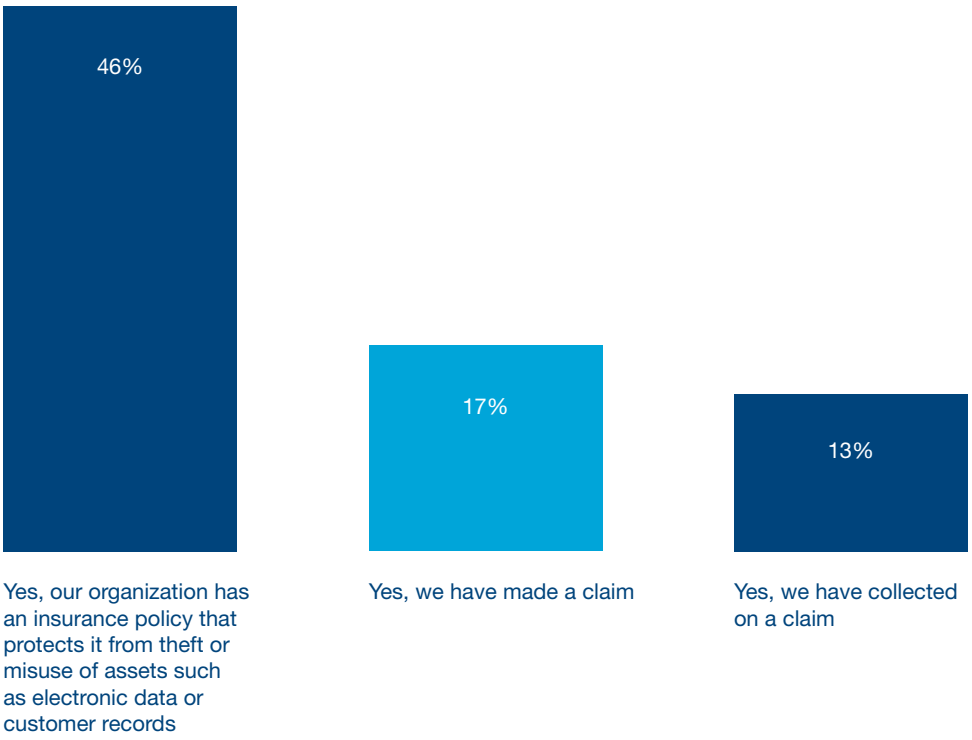
Source: The 2011 Global State of Information Security Survey®

Finding #14. A newly popular tool in the CISO's arsenal? Insurance.

Strategies in countering information security risks continue to emerge. For the first time this year, we asked respondents whether their organization has an insurance policy that protects it from theft or misuse of assets such as electronic data or customer records.

Almost half—46%—said "yes". And more than a few have made a claim (17%) and collected on it (13%). We expect to see these numbers rise significantly over the next several years. (Figure 16)

Figure 16: Percentage of all survey respondents reporting on the following insurance-related issues. [13]



[13] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

VI. Regional trends: A changing of the guard

Finding #15
With confidence, persistence and momentum, Asia lines up on the runway to become the new global leader in information security.

Finding #16
With more caution and restraint—and without the same promise of growth that Asia expects—North America idles its engines.

Finding #17
South America presses the gas pedal and the brakes at the same time, while Europe displays a marked lack of direction and urgency.

Finding #15. With confidence, persistence and momentum, Asia lines up on the runway to become the new global leader in information security.

After chasing North America for several years, Asia now reports higher maturity levels across more capabilities than any other world region.

Pick your metric. Asian respondents point to "client requirement" as among the leading justifications for security spending in far greater numbers than do those in any other world region. They are more likely to acknowledge that the increased risk environment inherent in current economic conditions has increased the role and importance of the security function. They're singularly more focused on data protections than those in other regions. And they are more progressive at addressing emerging practices—such as employing dedicated security personnel to support internal business departments and implementing security technologies supporting Web 2.0 exchanges.

At the same time, while Asian companies are pursuing comparable strategies to meet their security objectives in the context of harsher economic conditions, they're doing so with significantly more vigor and energy. For example, the enthusiasm with which Asian respondents consider strengthening governance, risk and compliance capabilities to be a "top priority," "very important" or "important" (75%) stands in marked contrast to the responses from South America (70%), North America (66%) and Europe (56%).

Just a blip in the multiyear trend lines? No. Quite the contrary. Asia has been doggedly plowing significant resources into information security programs for several years.

And Asia has momentum. Asian respondents are much more optimistic that security spending will increase in the months ahead than their regional counterparts worldwide. Soon Asia will lead the world in information security. Next year? The year after? Asia is just picking the runway. (Figures 17 and 18)

Finding #16. With more caution and restraint—and without the same promise of growth that Asia expects—North America idles its engines.

In acute contrast to Asia's advances in information security—and its more vigorous focus on strategic issues such as alignment of security with the business and the crucial need to protect data—North America has chosen to "gear down" on its investments in information security over the past year and look after its financial resources.

The writing is on the wall. Most of North America's maturity levels for information security capabilities have remained flat or declined over the past 12 months.

Although few in number, there were some bright spots worth noting. These include North American advances in embracing enterprise security management software and gains in improving the impact that virtualization has had on the information security function.

Remember, though, that the "gas" in the North American car isn't the same. Where Asian executives point proactively to "client requirement" as the leading justification for security spending, North American managers look reactively first to legal and regulatory mandates.

That's quite revealing—and perhaps a bit prophetic. In a few years, we may collectively look back on the first decade of this century and agree that in its adolescence, information security responded to a "stick"—regulation—as evidenced by North American leadership in the function through 2009. But as information security matured into a fully integrated business function with a guaranteed seat at the management table, the "carrot" proved the primary driver—client requirements and the revenue-enhancing role that security can play when it's truly aligned with the business. And we may well point to Asia's dominance in the function, first manifested in 2009 and 2010, as the first step in a new evolutionary phase for the function. (Figures 17 and 18)

Finding #17. South America presses the gas pedal and the brakes at the same time, while Europe displays a marked lack of direction and urgency.

Unlike Asia, which appears to have almost "shrugged off" many of the global economy's short-term impacts on information security, South America's focus on the function over the past year has been more volatile—and conflicted. On the one hand, South America stands right behind the Middle East and Africa as the regions most likely to defer security-related initiatives or reduce budgets for capital and operating expenditures—a sign that the flags of financial caution are flying high in these areas of the world. On the other, South Americans nearly rival Asians in their optimism that information security spending will increase over the next 12 months.

At the same time, in a year when every other global region is posting double-digit gains in concern that business partners and suppliers have been weakened by economic conditions, South America's anxiety on this point has actually declined. That's a worrisome sign given, for example, that only 28% of South Americans say their organization conducts due diligence of third parties handling the personal data of customers and employees.

In Europe, the focus on information is far more muted. Europe now trails other regions in maturity across most security capabilities. Although it is pursuing comparable strategies in addressing the impacts of the economic conditions—such as prioritizing security investments based on risk—it is doing so at a much lower level of commitment than its regional counterparts elsewhere in the world. Like North America, Europe continues to suffer poor visibility into security events and, as a result, may be unaware of the true impact of events on the business. And while 68% of European respondents say their organization places a high level of importance on protecting sensitive customer information, the responses from other global regions (Asia, 80%; North America, 80%; South America, 76%) reflect more conviction, direction and urgency. (Figures 17 and 18)

Figure 17: Differences in regional information security practices. [14]

	Asia	North America	South America	Europe
A leading driver of security spending: Economic conditions	53%	55%	51%	41%
A leading driver of security spending: Business continuity	50%	42%	35%	29%
A leading driver of security spending: Company reputation	41%	33%	37%	28%
One of the leading justifications for security: Legal/regulatory requirement	45%	55%	35%	35%
One of the leading justifications for security: Potential liability/exposure	45%	50%	32%	25%
One of the leading justifications for security: Client requirement	52%	37%	39%	29%
Security spending will increase or stay the same	86%	71%	81%	68%
View protecting sensitive customer information “important/extremely important”	80%	80%	76%	68%
Use enterprise security management software	49%	42%	41%	34%
Have accurate inventory of where sensitive data stored	42%	40%	33%	24%
Have an overall information security strategy	68%	73%	58%	60%
Have established security baselines for partners and customers	46%	55%	47%	39%
Have dedicated security personnel supporting internal business departments	56%	45%	51%	38%
Have handheld/portable device security standards	52%	47%	41%	36%
Encrypt removable media	59%	44%	53%	43%
Use tools to discover unauthorized devices	56%	56%	52%	45%
Use data leakage prevention (DLP) tools	50%	46%	41%	40%
Have security technologies supporting Web 2.0 exchanges	48%	36%	43%	32%
Number of security incidents in the past 12 months: Unknown	14%	37%	19%	29%
Type of security incidents: Unknown	22%	43%	35%	40%
Likely source of incidents: Unknown	26%	44%	31%	41%
Business impacts of security incidents: Financial losses	49%	39%	45%	32%
Business impacts of security incidents: Intellectual property theft	35%	35%	29%	29%
Business impacts of security incidents: Brand/reputation compromised	35%	32%	22%	28%
Conduct enterprise risk assessment at least twice a year	41%	28%	42%	33%
Continuously prioritize information assets according to their risk level	24%	16%	20%	16%
Have a centralized security information management process	52%	57%	44%	40%

[14] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.

Source: The 2011 Global State of Information Security Survey®

Figure 18: Differences among regional perceptions of the impacts of the economic downturn on the information security function. [15]

	Asia	North America	South America	Europe
Increased risk environment has elevated the role and importance of the information security function	65%	53%	56%	45%
The regulatory environment has become more complex and burdensome	62%	58%	52%	50%
Cost reduction efforts make adequate security more difficult to achieve	53%	53%	55%	43%
Our business partners have been weakened by the downturn	57%	54%	48%	48%
Our suppliers have been weakened by the downturn	55%	52%	46%	46%
Risks to the company's data have increased due to employee layoffs	46%	39%	43%	38%
Threats to the security of our information assets have increased	48%	50%	41%	33%

[15] Respondents who answered either "agree" or "strongly agree."

Source: The 2011 Global State of Information Security Survey®

What this means for your business

Learn from the downturn. And make crucial changes.

But also be among the first to face forward.

It's an uncertain year, and security hangs in the balance. On the one hand, the flags of caution are prominent:

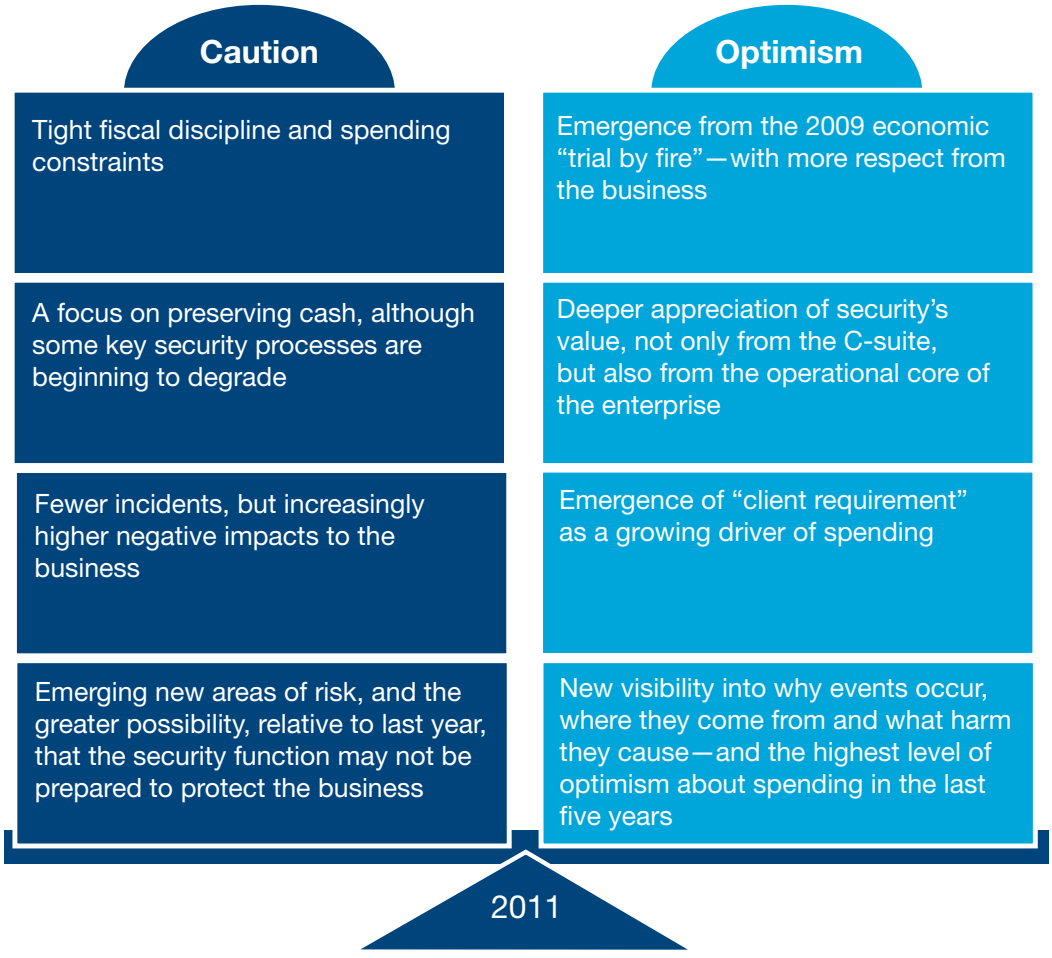
- Tight fiscal discipline and spending constraints
- A focus on preserving cash, although some key security processes are beginning to degrade
- Fewer incidents, but increasingly higher negative impacts to the business
- Emerging new areas of risk and the greater possibility, relative to last year, that the security function may not be prepared to protect the business

On the other hand, the signs of optimism—and growing functional maturity—are impossible to miss:

- Emergence from the 2009 economic "trial by fire" with more respect from the business
- Deeper appreciation of security's value, not only from the C-suite—but also from the operational core of the enterprise
- Emergence of "client requirement" as a growing driver of spending
- New visibility into why events occur, where they come from and what harm they cause—and the highest level of optimism about spending in the last five years

What does this mean for your business? Learn from the downturn. And make crucial changes. But also be the first among your competitors to face forward and strategically position your information security function to support your performance in the years ahead.

Figure 19: It's an uncertain year—and security hangs in the balance.



pwc.com/giss2011

For more information,
please contact:

Gary Loveland
Principal, National Security Leader
949.437.5380
gary.loveland@us.pwc.com

Mark Lobel
Principal
646.471.5731
mark.a.lobel@us.pwc.com

or visit:
www.pwc.com/giss2011

This publication is printed on Mohawk Options PC.
It is a Forest Stewardship Council (FSC) certified
stock using 100% post-consumer waste (PCW) fiber
and manufactured with renewable, non-polluting
wind-generated electricity.

Recycled paper